

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please amend the claims as follows:

1. (Currently Amended) An apparatus comprising:

~~a network interface module to connect the apparatus to a network;~~

~~a packet capture module to intercept packets being transmitted on the network;~~

an object assembly module to reconstruct flows representing objects being transmitted on ~~the a~~ network from ~~the intercepted~~ packets, the packets associated with a document that includes the objects, wherein the document is captured based on a capture rule that specifies the objects, and wherein a determination is made as to whether to discard or to store the objects of the document;

an object classification module to determine a type of content of the objects and to reconstruct the objects from the flows;

an object store module to store the objects, wherein a location for storing the objects is determined based at least in part on the type of content for each of the objects, wherein the object store module comprises a content store to store the objects and a tag store to index the objects stored in the object store; and

a user interface to enable a user to search objects stored in the object store module, wherein the objects are searched based on a query, which includes search criteria used to identify selected objects that match the search criteria, wherein a particular search is scheduled for a recurring time interval and includes a particular search query with selected terms, and wherein certain results of the particular search trigger an alarm in a form of an e-mail message to be sent to an administrator.

2. (Original) The apparatus of claim 1, wherein the object assembly module comprises a reassembler to assemble the intercepted packets into flows.

3. (Original) The apparatus of claim 2, wherein the object assembly module further comprises a protocol demultiplexer to sort the assembled flows by protocol.

4. (Original) The apparatus of claim 3, wherein the object assembly module further comprises a protocol classifier to extract the objects from the sorted assembled flows.

5. (Original) The apparatus of claim 1, wherein the object classification module determines whether objects are stored in the object store or discarded based on one or more capture rules.

6. (Original) The apparatus of claim 5, wherein the capture rules are user-configurable through the user interface.

7. (Cancelled)

8. (Original) The apparatus of claim 1, wherein the object classification module determines the type of content of each object using a signature of each object.

9. (Original) The apparatus of claim 1, wherein the user interface comprises a graphical user interface.

10. (Cancelled)

ATTORNEY DOCKET NO.  
006897.P001  
Confirmation No. 8139

PATENT APPLICATION  
10/815,240

4

11. (Currently Amended) The apparatus of ~~claim 10~~ Claim 1, wherein the content store comprises a canonical storage, and the tag store comprises a database.

12. (Currently Amended) A method comprising:

intercepting data being transmitted on a network;

reconstructing flows of objects being transmitted on the a network from the intercepted data;

classifying the reconstructed objects by content type, the data associated with a document that includes the objects, wherein the document is captured based on a capture rule that specifies the objects, and wherein a determination is made as to whether to discard or to store the objects of the document;

creating a tag to describe each reconstructed object;

storing the classified objects and tags; and

indexing the stored objects to enable searching of the stored objects via the tags, wherein the content type of the objects is used in the indexing, and wherein the objects are searched based on a query, which includes search criteria used to identify selected objects that match the search criteria, wherein a particular search is scheduled for a recurring time interval and includes a particular search query with selected terms, and wherein certain results of the particular search trigger an alarm in a form of an e-mail message to be sent to an administrator.

13. (Previously Presented) The method of claim 12, wherein reconstructing the objects comprises:

sorting the intercepted data into packets; and

sorting the assembled flows by protocol.

14. (Original) The method of claim 12, further comprising determining whether each object is to be stored based on a set of one or more capture rules.

15. (Original) The method of claim 12, further comprising receiving a query over the stored objects.

16. (Original) The method of claim 15, further comprising searching the indexed objects, and retrieving objects matching the query.

17. (Currently Amended) A machine-readable storage medium having stored thereon data representing instructions that, when executed by a processor, cause the processor to perform operations comprising:

intercepting data being transmitted on a network;

reconstructing flows of objects being transmitted on the a network from the intercepted data;

classifying the reconstructed objects by content type, the data associated with a document that includes a plurality of objects that identify characteristics of the document, wherein the document is captured based on a capture rule that specifies the objects, and wherein a determination is made as to whether to discard or to store the objects of the document;

creating a tag to describe each reconstructed object;

storing the classified objects and tags; and

indexing the stored objects to enable searching of the stored objects via the tags, wherein the content type of the objects is used in the indexing, and wherein the objects are searched based on a query, which includes search criteria used to identify selected objects that match the search criteria, wherein a particular search is scheduled for a recurring time interval and includes a particular search query with selected terms, and wherein certain results of the particular search trigger an alarm in a form of an e-mail message to be sent to an administrator.

18. (Previously Presented) The machine-readable storage medium of claim 17, wherein reconstructing the objects comprises:

sorting the intercepted data into packets; and

sorting the assembled flows by protocol.

19. (Previously Presented) The machine-readable storage medium of claim 17, wherein the instructions further cause the processor to determine whether each object is to be stored based on a set of one or more capture rules.

20. (Previously Presented) The machine-readable storage medium of claim 17, wherein the instructions further cause the processor to receive a query over the stored objects, search the indexed objects in response to the query, and retrieve objects matching the query.